Die europäische NIS2-Direktive

Die Ende 2022 beschlossene NIS2-Direktive muss bis Oktober 2024 in allen EU-Mitgliedsstaaten in nationale Gesetzgebung überführt werden. Bis zum Sommer wird geklärt werden, welche Unternehmen in Deutschland tatsächlich betroffen sind. Darauf basierend soll bis zum Jahresende das Umsetzungsgesetz beschlossen werden. Dem EU-Richtlinien-Text entsprechend könnten in Deutschland bis zu 40.000 Unternehmen und vergleichbare Einrichtungen in den Geltungsbereich fallen und von der Umsetzung ambitionierter Anforderungen und Pflichten – inklusive empfindlichen Geldbußen bei Nicht-Kooperation - betroffen sein. Im Folgenden gehen wir in Kürze auf die wichtigsten Eckpunkte ein.

GELTUNGSBEREICH (ARTIKEL 2 & 3)

Die Direktive führt die Unterscheidung von **wesentlichen** und **wichtigen** Sektoren[1] fort. Alle Unternehmen innerhalb dieser Sektoren müssen die Anforderungen und Plichten umsetzen, wenn sie gemäß 2003/361/EC[2] als **mittel** bzw. **groß** gelten oder historisch bereits als KRITIS erfasst wurden. Zusätzlich werden unabhängig von ihrer Größe digitale Infrastruktur und Spezialfälle nach Kritikalität[3] inkludiert.

ANFORDERUNGEN (ARTIKEL 21)

Die in den Geltungsbereich fallenden Unternehmen müssen technische, organisatorische und physische Maßnahmen auf Basis eines geeigneten Risikomanagements zur Absicherung identifizieren und umsetzen. Diese beinhalten bekannte Themen aus: Informationssicherheitsmanagementsystemen (ISMS), Business Continuity Managementsystemen (BCM), Incident Management, Lieferkettenmanagement, Schwachstellenmanagement, Pentesting und technischen Audits, Sensibilisierung und Schulung, Verschlüsselung, Zugriffsmanagement und Authentifizierungslösungen. Exakte Vorgaben über die genaue Umsetzung bestehen bisher nicht.

PFLICHTEN (ARTIKEL 23)

Bei signifikanten[4] Sicherheitsvorfällen müssen Unternehmen die zuständigen Behörden innerhalb von 24 Stunden mit einer Erstmeldung informieren. Innerhalb von 72 Stunden hat eine präzisierte Vorfallsmeldung stattzufinden, auf welche bei erfolgreicher Vorfallsbehandlung innerhalb von einem Monat ein Abschlussbericht zu folgen hat. Ist die Vorfallsbehandlung innerhalb von einem Monat nicht erfolgreich, ist eine Fortschrittsmeldung zu leisten. Zu dieser kann die zuständige Behörde einen präziseren Zwischenbericht anfordern, welchen die Einrichtung dann auszustellen hat. Nach erfolgreicher Bereinigung hat dann wiederum ein Abschlussbericht zu erfolgen.

[1] Als **wesentlich** wurden elf Sektoren deklariert: Digitale Infrastruktur, IT-Service Management, Energie, Transport, Trinkwasser, Gesundheit, Finanzmärkte, Banken, *Öffentliche Verwaltung*, *Abwasser* und *Raumfahrt* (Kursive Sektoren sind unter NIS2 neu erfasst).
Wichtig sind sieben Sektoren: Post und Kurierdienste, *Forschung*, *Abfallwirtschaft*, *Lebensmittel*, *Chemikalien*, *Verarbeitendes Gewerbe* und *Digitale Dienste*.

[2] Als **mittel** gelten Unternehmen mit 50-250 Mitarbeitern und einem Umsatz zwischen 10 und 50 Mio. Euro oder einer Bilanz kleiner 43 Mio. Euro; als **groß** gelten Unternehmen mit mehr als 250 Mitarbeitern und einem Umsatz höher 50 Mio. Euro oder einer Bilanz größer 43 Mio. Euro.

[3] Spezialfälle können entweder direkt von Mitgliedsstaaten definiert werden oder sind durch eine Sonderstellung, wie grenzüberschreitende Relevanz, besondere Kritikalität oder nationale Monopolstellung, geprägt.

[4] Als signifikant gelten Sicherheitsvorfälle, welche eine schwerwiegende Betriebsstörung, finanzielle Verluste oder materielle bzw. immaterielle Schäden einer (juristischen) Person verursachen.

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

HISOLUTIONS

AUFSICHTSMASSNAHMEN (ARTIKEL 32 & 33)

Um die Umsetzung zu kontrollieren, erhalten die zuständigen Behörden eine Reihe von Befugnissen. Diese beinhalten für **wesentliche** und **wichtige** Einrichtungen die folgenden Punkte:

- Vor-Ort-Kontrollen, auch unangekündigt als Stichprobe;
- Anordnen von Sicherheitsprüfungen durch unabhängige Dritte;
- Ad-hoc-Prüfungen basierend auf Sicherheitsvorfällen oder gemeldeten Verstößen gegen die nationale NIS2-Umsetzung (entfällt bei **wichtigen** Einrichtungen);
- Durchführung von Sicherheitsscans;
- Verpflichtungen zur Übermittlung von Informationen bzgl. Risikomanagementmaßnahmen;
- Zugang zu Daten, Dokumenten und Informationen zur Erfüllung der Aufsichtsaufgaben seitens der Behörden;
- Nachweise für die Umsetzung von Cybersicherheitskonzepten.

DURCHSETZUNGSMASSNAHMEN (ARTIKEL 32, 33 & 34)

Falls die Anforderungen und Pflichten nicht umgesetzt werden, können die zuständigen Behörden Maßnahmen zur Durchsetzung veranlassen. Dazu gehören:

- Warnungen über Verstöße an die Öffentlichkeit;
- Verbindliche Anweisungen zu Umsetzung von Maßnahmen;
- Verbindliche Anweisungen Verhalten einzustellen;
- Spezifische Anweisungen, Anforderungen und Pflichten umzusetzen;
- Verpflichten der Einrichtungen, Betroffene von Sicherheitsvorfällen zu informieren;
- Verpflichtung, Empfehlungen aus unabhängigen Sicherheitsprüfungen per Frist umzusetzen;
- Benennung von internen Überwachungsbauftragten zu Anforderungen und Pflichten (entfällt bei **wichtigen** Einrichtungen);
- Vorgaben zur Veröffentlichung von Verstößen gegen NIS2;
- Verhängung von Geldbußen für **wesentliche** Unternehmen in Höhe von mindestens 10 Mio. Euro bzw. 2 % des globalen Umsatzes und für **wichtige** Unternehmen in Höhe von mindestens 7 Mio. Euro bzw. 1,4 % des globalen Umsatzes. Die Strafen sollen bei bei Nicht-Erfüllung von Anforderungen, Pflichten und Durchsetzungsmaßnahmen zu verhängen sein.

UNKLARHEITEN

Wie die Richtlinie in Deutschland und anderen Mitgliedsstaaten in nationales Recht überführt wird ist derzeit ungewiss (Stand Mitte März 2023). Außerdem abzuwarten sind die erwarteten Maßstäbe der Behörden für die Implementierung der Anforderungen und Pflichten. Selbiges gilt für einzelne Unterpunkte hinsichtlich der Umsetzung bei denen gängige Best Practices nicht mit der gesamten IT-Lieferkette der in den Geltungsbereich fallenden Unternehmen skalieren.

ÜBER DIE HISOLUTIONS AG

Die HiSolutions AG ist ein führender deutscher Beratungsdienstleister in den Bereichen Cyber Security, Informationssicherheit, Business Continuity, Krisenmanagement und Wirtschaftsschutz. Dabei vereinen wir strategische Beratungskompetenz mit fundierten methodischen Vorgehensweisen und technischer Expertise. Unsere Berater engagieren sich seit 30 Jahren in der Planung, Umsetzung und Überprüfung strategischer, organisatorischer, physischer, personeller sowie technischer Sicherheitsmaßnahmen und gehören so zu den erfahrensten und renommiertesten Sicherheitsspezialisten im deutschsprachigen Raum.

Ihr Ansprechpartner

Andre Windsch
Managing Consultant

info@hisolutions.com
Fon +49 30 533 289-0